

09/402144

420 Rec'd PCT/PTO 29 SEP 1999

1

Beschreibung

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente
5 gruppiert sind

Bei der digitalen Kommunikation, d.h. beim Austausch digitaler Daten ist es oftmals wünschenswert, die Übertragung der elektronischen Daten hinsichtlich verschiedenster Aspekte ab-
10 zusichern.

Ein sehr bedeutender Aspekt ist der Schutz der zu übertragenden digitalen Daten gegen unerlaubte Modifikation, die sog. Sicherung der Integrität der Daten.

15

Aus [1] ist zum Schutz gegen unerlaubte Modifikation digitaler Daten die sog. kryptographische Prüfsumme bekannt, z.B. die digitale Signatur. Das in [1] beschriebene Verfahren basiert auf der Bildung eines Hashwertes aus den digitalen
20 Nutzdaten und der anschließenden kryptographischen Bearbeitung des Hashwertes mit einem kryptographischen Schlüssel. Das Ergebnis ist eine kryptographische Prüfsumme. Zur Überprüfung der Integrität wird mit einem entsprechenden kryptographischen Schlüssel die inverse kryptographische Operation
25 auf die gebildete Prüfsumme durchgeführt und das Ergebnis mit dem erneut aus den Nutzdaten berechneten Hashwert verglichen. Bei Übereinstimmung der ermittelten Hashwerte ist die Integrität der Nutzdaten gewährleistet.

30 Diese bisher übliche Vorgehensweise bedingt, daß die kompletten Nutzdaten auf Empfängerseite in identischer Reihenfolge, wie sie bei der Bildung des Hashwertes vorlagen, vorliegen müssen, da sonst die Hashwertbildung zu einem fehlerhaften Wert führt. Oftmals ist es jedoch bei der digitalen Kommuni-
35 kation üblich, die zu übertragenden Nutzdaten aufgrund von Protokollrandbedingungen in kleinere Datensegmente, die auch als Datenpakete bezeichnet werden, zu unterteilen und zu

übertragen. Die Datensegmente sind oftmals nicht an eine definierte Reihenfolge gebunden oder ein definiertes sequentielles Eintreffen der Datensegmente kann nicht garantiert werden. Bei dem Verfahren aus [1] ist es also erforderlich, daß
5 die kompletten Nutzdaten auf Empfängerseite, d.h. nach der Übertragung der Datensegmente wieder in der Reihenfolge, in der sie ursprünglich gesendet wurden, zusammengesetzt werden. Die zu übertragenden Daten können ausschließlich in dieser Reihenfolge verifiziert werden. Dies bedeutet jedoch oft ei-
10 nen erheblichen zusätzlichen Aufwand zur Flußkontrolle der Datensegmente, soweit dies überhaupt im Rahmen des verwendeten Protokolls möglich ist.

Aus [2] sind Grundlagen über kommutative Verknüpfungen be-
15 kannt. In [2] ist ferner eine allgemeine Definition für kommutative Verknüpfungen angegeben. Anschaulich ist unter einer kommutativen Verknüpfung eine Verknüpfung zu verstehen, bei der die Reihenfolge der Einzelverknüpfungen unwichtig ist und jede Reihenfolge der Einzelverknüpfung immer zu der gleichen
20 Gesamtverknüpfung führt. Eine kommutative Verknüpfung kann beispielsweise eine EXOR-Verknüpfung, eine additive Verknüpfung oder auch eine multiplikative Verknüpfung sein.

Aus [3] sind ein Verfahren und eine Vorrichtung zur Erzeugung
25 von Prüfkodesegmenten auf das Auftreten von Quelldaten hin und zur Ermittlung von Fehlern in den Quelldaten bekannt.

Somit liegt der Erfindung das Problem zugrunde, Verfahren und Anordnungen zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in mehrere Datenseg-
30 mente gruppiert sind, anzugeben, bei der eine Flußkontrolle für die einzelnen Datensegmente nicht mehr erforderlich ist.

Das Problem wird durch das Verfahren gemäß Patentanspruch 1,
35 durch das Verfahren gemäß Patentanspruch 2, durch das Verfahren gemäß Patentanspruch 3, durch die Anordnung gemäß Patent-

anspruch 11, durch die Anordnung gemäß Patentanspruch 12 sowie durch die Anordnung gemäß Patentanspruch 13, gelöst.

- Bei dem Verfahren gemäß Patentanspruch 1 wird für digitale
- 5 Daten, die in mehrere Datensegmente gruppiert sind, für jedes Datensegment eine erste Segmentprüfsumme gebildet. Die gebildeten ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft.
- 10 Bei dem Verfahren gemäß Patentanspruch 2 wird eine vorgegebene erste kommutative Prüfsumme, die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, überprüft. Dies erfolgt dadurch, daß für jedes Datensegment eine
- 15 zweite Segmentprüfsumme gebildet wird und durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.
- 20 Bei dem Verfahren gemäß Patentanspruch 3 zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in Datensegmente gruppiert sind, wird für jedes Datensegment eine erste Segmentprüfsumme gebildet und die ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Für
- 25 jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, werden zweite Segmentprüfsummen gebildet und durch kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.
- 30

- Die Anordnung gemäß Patentanspruch 11 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Daten-
- 35 segment eine Segmentprüfsumme gebildet wird, und daß durch eine kommutative Verknüpfung der Segmentprüfsummen die erste kommutative Prüfsumme gebildet wird.

- Die Anordnung gemäß Patentanspruch 12 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Daten-segment eine zweite Segmentprüfsumme gebildet wird, durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird, und die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.
- 10 Die Anordnung gemäß Patentanspruch 13 weist eine Recheneinheit auf, die derart eingerichtet ist, daß folgende Verfahrensschritte durchgeführt werden:
- a) für jedes Datensegment wird eine Segmentprüfsumme gebildet,
 - 15 b) durch eine kommutative Verknüpfung der Segmentprüfsummen wird die erste kommutative Prüfsumme gebildet,
 - c) für jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, wird eine zweite Segmentprüfsumme gebildet,
 - 20 d) durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet, und
 - e) die zweite kommutative Prüfsumme wird mit der ersten kommutativen Prüfsumme auf Übereinstimmung überprüft.
- 25 Ein erheblicher Vorteil der Verfahren sowie der Anordnungen ist darin zu sehen, daß durch Verwendung einer kommutativen Verknüpfung für einzelne Prüfsummen der Datensegmente eine Flußkontrolle für die Reihenfolge der einzelnen Datensegmente
- 30 nicht mehr erforderlich ist.
- Es ist ferner nicht mehr erforderlich, die kompletten Nutzdaten wieder in der ursprünglichen Reihenfolge, in der die erste kommutative Prüfsumme gebildet wurde, zusammenzusetzen.
- 35 Die Reihenfolge der einzelnen Datensegmente bei der Bildung der kommutativen Prüfsumme ist nicht mehr von Bedeutung.

Werden die digitalen Daten zwischen zwei Anordnungen übertragen, so ist ein weiterer Vorteil der Verfahren darin zu sehen, daß die Überprüfung der Integrität schon begonnen werden kann, bevor alle Datensegmente empfangen worden sind, da es nicht mehr erforderlich ist, die ursprüngliche Reihenfolge bei der Bildung der ersten Prüfsumme beizubehalten. Dies führt zu einem Zeitersparnis bei der Überprüfung der Integrität der Daten.

10 Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden.

15 Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Es ist vorteilhaft, die erste kommutative Prüfsumme unter Verwendung mindestens einer kryptographischen Operation kryptographisch abzusichern.

Durch diese Weiterbildung wird erreicht, daß die kryptographische Sicherheit der Daten erheblich erhöht wird. Eine kryptographische Operation in diesem Sinne ist beispielsweise die Verschlüsselung der ersten kommutativen Prüfsumme mit einem symmetrischen oder auch mit einem asymmetrischen Verschlüsselungsverfahren, wodurch eine kryptographische Prüfsumme gebildet wird. Auf Empfängerseite wird das inverse kryptographische Verfahren zu dem kryptographischen Verfahren durchgeführt, um die kryptographische Sicherheit zu gewährleisten.

35 Zur Bildung einer Prüfsumme, wie sie im Rahmen des Dokuments zu verstehen ist, sind verschiedene Möglichkeiten bekannt: -eine Prüfsumme kann durch Bildung von Hashwerten für die einzelnen Datensegmente gebildet werden;

- die Prüfsummen können auch durch sog. zyklische Codes (Cyclic Redundancy Check, CRC) gebildet werden;
- es kann ferner eine kryptographische Einwegfunktion zur Bildung der Prüfsummen für die Datensegmente verwendet werden.

Die Verfahren können vorteilhaft in verschiedenen Anwendungsszenarien eingesetzt werden.

- 10 Die Verfahren können sowohl bei der Übertragung digitaler Daten zum Schutz vor Manipulation der Daten eingesetzt werden als auch bei der Archivierung digitaler Daten in einem Rechner, in dem die erste kommutative Prüfsumme gebildet wird, und zusammen mit den zu archivierenden Daten abgespeichert
- 15 wird. Die erste kommutative Prüfsumme kann bei dem Laden der digitalen Daten aus dem Archivspeicher überprüft werden, um eine Manipulation der archivierten Daten zu erkennen.

- Das Verfahren kann vorteilhaft für die Sicherung digitaler
- 20 Daten verwendet werden, deren Datensegmente nicht an eine Reihenfolge gebunden sind. Beispiele für solche Datensegmente sind paketerorientierte Kommunikationsprotokolle, z.B. Netzwerkmanagementprotokolle wie das Simple Network Management Protocol (SNMP) oder das Common Management Information Protocol
- 25 (CMIP).

- Im weiteren wird ein Ausführungsbeispiel der Erfindung anhand einer Figur näher erläutert. Auch wenn das Ausführungsbeispiel im weiteren anhand des Simple-Network-Management-
- 30 Protocols (SNMP) erläutert wird, so stellt dies keine Einschränkung der Verwendbarkeit des Verfahrens dar. Das Verfahren kann immer dann eingesetzt werden wenn es gilt, eine Integritätssicherung für digitale Daten zu gewährleisten, die in mehrere Datensegmente gruppiert sind.

Die Figur zeigt zwei Anordnungen, wobei von der ersten Anordnung Datensegmente zu der zweiten Anordnung übertragen werden.

- 5 In der Figur ist eine erste Rechneranordnung A1 symbolisch dargestellt, in der Datensegmente (D_i , $i = 1 \dots n$) gespeichert sind. Die Datensegmente D_i bilden zusammen die digitalen Daten, die auch als Nutzdaten bezeichnet werden, für die es gilt, die Integrität zu gewährleisten.

10

Sowohl die erste Rechneranordnung A1 als auch eine im weiteren beschriebene zweite Rechneranordnung A2 enthalten jeweils eine Recheneinheit R, die derart eingerichtet ist, daß die im weiteren beschriebenen Verfahrensschritte durchgeführt werden.

15

- In der ersten Anordnung A1 sind die Datensegmente D_i an Positionen P_i innerhalb des gesamten Datenstroms angeordnet. Für jedes Datensegment D_i wird eine erste Segmentprüfsumme PS_i unter Verwendung einer Prüfsummenfunktion PSF. Die einzelnen ersten Segmentprüfsumme PS_i werden durch eine kommutative Verknüpfung, wie sie in [2] definiert und beschrieben ist, zu einer ersten kommutativen Prüfsumme KP_1 verknüpft. Die kommutative Verknüpfung zwischen den einzelnen Prüfsummen PS_i sind in der Figur durch ein EXOR-Zeichen \oplus symbolisch dargestellt.

20

25

- Die erste kommutative Prüfsumme KP_1 wird einem kryptographischen Verfahren, einem symmetrischen oder asymmetrischen Verfahren, unter Verwendung eines ersten kryptographischen Schlüssels S unterzogen (Schritt 101). Das Ergebnis der kryptographischen Operation ist eine kryptographische Prüfsumme KP.

30

- 35 Sowohl die Datensegmente D_i als auch die kryptographische Prüfsumme KP werden über ein Übertragungsmedium, vorzugsweise eine Leitung oder auch eine logischen Verbindung, die in der

Fig. durch eine Kommunikationsverbindung UM symbolisch dargestellt ist, zu einer zweiten Anordnung A2 übertragen und dort empfangen.

- 5 Die sich überkreuzenden Pfeile der Datensegmente D_i in der Figur deuten an, daß durch die Übertragung der Datensegmente D_i diese in einer gegenüber der Reihenfolge in der ersten Anordnung A1 verschobenen Positionen P_j ($j = a \dots z$) empfangen werden.

10

- So wird ein Datensegment D_2 an der ersten Position P_1 in der zweiten Anordnung A2 als Datensegment D_a empfangen. Das Datensegment D_1 wird als Datensegment D_c in der zweiten Anordnung empfangen. Das Datensegment D_n wird als empfangenes Datensegment D_b in der zweiten Anordnung A2 an der zweiten Position P_2 empfangen.

15

- Entsprechend dem verwendeten Verfahren wird entweder mit dem ersten kryptographischen Schlüssel S bei Verwendung eines symmetrischen Verschlüsselungsverfahrens die inverse kryptographische Operation auf die kryptographische Prüfsumme KP ausgeführt oder bei Verwendung eines asymmetrischen kryptographischen Verfahrens unter Verwendung eines zweiten kryptographischen Schlüssels S' .

25

Das Ergebnis der inversen kryptographischen Operation (Schritt 102) ist bei korrekter Verschlüsselung und Entschlüsselung wiederum die erste kommutative Prüfsumme KP_1 .

- 30 Diese wird in der zweiten Anordnung A2 gespeichert. Für den Vergleich der nunmehr in permutierter Reihenfolge, verglichen mit der ursprünglichen Reihenfolge bei der Bildung der ersten kommutativen Prüfsumme KP_1 empfangenen Datensegmente D_j , werden wiederum unter Verwendung der gleichen Prüfsummenverfahren PSF zweite Segmentprüfsummen Ps_j für die empfangenen Datensegmente D_j gebildet.

35

Die sich ergebenden zweiten Prüfsummen PS_j werden wiederum kommutativ miteinander verknüpft zu einer zweiten kommutativen Prüfsummen $KP2$.

- 5 In einem weiteren Schritt 103 wird überprüft, ob die erste kommutative Prüfsumme $KP1$ mit der zweiten kommutativen Prüfsumme $KP2$ übereinstimmt.

10 Ist dies der Fall, so ist die Integrität der Datensegmente D_i und somit die Integrität der gesamten digitalen Daten gewährleistet (Schritt 104), wenn die verwendeten kryptographischen Verfahren bzw. die verwendeten Verfahren zur Prüfsummenbildung die entsprechende kryptographische Sicherheit gewährleisten.

15 Stimmen die erste kryptographische Prüfsumme $KP1$ und die zweite kryptographische Prüfsumme $KP2$ nicht miteinander überein, so würde die Integrität der Datensegmente D_i verletzt und es wird eine Manipulation der Daten festgestellt und vorzugsweise einem Benutzer des Systems gemeldet.

20

Die Protokolldateneinheiten PDU (Protocol Data Units) sind in SNMP derart aufgebaut, daß in der Nutzdateninformation (sog. Variable Bindings) eine Liste von Objekten

25 (Objektidentifikatoren, OID/Value-Pairs) enthalten sein kann. Die Reihenfolge der Objekte innerhalb einer PDU ist dabei nicht festgelegt, so daß eine Permutation der Objekte bei der Übertragung der PDUs zwischen der ersten Anordnung $A1$ und der zweiten Anordnung $A2$ auftreten kann. Durch die Erfindung wird

30 es nunmehr möglich, über alle Objekte einer SNMP-PDU eine einzige kryptographische Prüfsumme zu bilden, ohne daß die Reihenfolge der Objekte bzw. der PDUs berücksichtigt werden muß.

35 Im weiteren werden Alternativen zu dem oben beschriebenen Ausführungsbeispiel erläutert.

Das Verfahren zur Bildung der Prüfsumme PSF kann beispielsweise ein Verfahren zur Bildung von Hashwerten sein. Es kann aber auch Verfahren zur Bildung zyklischer Codes (Cyclic-Redundancy-Check, CRC) unter Verwendung rückgekoppelter Schieberegister eingesetzt werden. Auch können kryptographische Einwegfunktionen zur Bildung der Prüfsummen PS_i bzw. PS_j verwendet werden.

Ferner kann die kommutative Verknüpfung zusätzlich die Eigenschaft der Assoziativität aufweisen.

Sowohl das Verfahren zur Bildung der Prüfsumme als auch das Verfahren zur Überprüfung einer Prüfsumme können unabhängig voneinander durchgeführt werden. Es kann jedoch auch gemeinsam das Verfahren zur Bildung der Prüfsumme und das Verfahren zur Überprüfung der Prüfsumme durchgeführt werden.

Es ist ferner vorgesehen, keine Übertragung digitaler Daten vorzunehmen, sondern die digitalen Daten zu archivieren, d.h. in der ersten Anordnung A1 zu speichern, gemeinsam mit der ersten kommutativen Prüfsumme KP_1 . Bei der Wiederverwendung der archivierten Daten, d.h. beim Laden der Datensegmente D_i aus dem Speicher der ersten Anordnung A1 wird dann das Verfahren zur Überprüfung der ersten kommutativen Prüfsumme KP_1 , wie es oben beschrieben wurde, durchgeführt. Somit können die erste Anordnung A1 und die zweite Anordnung A2 identisch sein.

Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden. Dadurch wird es möglich, eine Prüfsumme zu bilden und zu überprüfen, ohne daß die Reihenfolge der Datensegmente berücksichtigt werden muß.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert:

- 5 [1] W. Stallings, Sicherheit in Netzwerk und Internet,
Prentice Hall, ISBN 3-930436-29-9, S. 203-223, 1995
- [2] K.-H. Kiyek und F. Schwarz, Mathematik für Informatiker,
Teubner Verlag, ISBN 3-519-03277-X, S. 11-13, 1989
- 10 [3] DE-OS 2 048 365

Patentansprüche

1. Verfahren zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (D_i , $i = 1 \dots n$) gruppiert sind, durch einen Rechner,
 - a) bei dem für jedes Datensegment (D_i) eine Segmentprüfsumme (PS_i) gebildet wird, und
 - b) bei dem durch eine kommutative Verknüpfung (\oplus) der Segmentprüfsummen (PS_i) die erste kommutative Prüfsumme (KP1) gebildet wird.
2. Verfahren zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme (KP1), die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, durch einen Rechner,
 - a) bei dem für jedes Datensegment (D_j , $j = a \dots z$) eine zweite Segmentprüfsumme (PS_j) gebildet wird,
 - b) bei dem durch eine kommutative Verknüpfung (\oplus) der zweiten Segmentprüfsummen (PS_j) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
 - c) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.
3. Verfahren zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (D_i , $i = 1 \dots n$) gruppiert sind, durch einen Rechner,
 - a) bei dem für jedes Datensegment (D_i) eine Segmentprüfsumme (PS_i) gebildet wird,
 - b) bei dem durch eine kommutative Verknüpfung (\oplus) der Segmentprüfsummen (PS_i) die erste kommutative Prüfsumme (KP1) gebildet wird,
 - c) bei dem für jedes Datensegment (D_j , $j = a \dots z$) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PS_j) gebildet wird,

d) bei dem durch eine kommutative Verknüpfung (\oplus) der zweiten Segmentprüfsummen (Ps_j) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

5 e) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
10 bei dem die Segmentprüfsummen (Psi , Ps_j) nach mindestens einer der folgenden Arten gebildet werden:

- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

15 5. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

20 6. Verfahren nach Anspruch 5,
bei dem die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

25 7. Verfahren nach Anspruch 5,
bei dem die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

30 8. Verfahren nach einem der Ansprüche 1 bis 7,
bei dem die kommutative Verknüpfung (\oplus) die Eigenschaft der Assoziativität aufweist.

35 9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.

5 11. Anordnung zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (D_i , $i = 1 \dots n$) gruppiert sind, mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (D_i) eine Segmentprüfsumme (PS_i)
10 gebildet wird, und
b) durch eine kommutative Verknüpfung (\oplus) der Segmentprüfsummen (PS_i) die erste kommutative Prüfsumme (KP1) gebildet wird.

15 12. Anordnung zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme (KP1), die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (D_j , $j = a \dots z$) eine zweite Segmentprüfsumme (PS_j) gebildet wird,
20 b) durch eine kommutative Verknüpfung (\oplus) der zweiten Segmentprüfsummen (PS_j) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
c) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.
25

13. Anordnung zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (D_i , $i = 1 \dots n$) gruppiert sind,
30 mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (D_i) eine Segmentprüfsumme (PS_i) gebildet wird,
b) durch eine kommutative Verknüpfung (\oplus) der Segmentprüfsummen (PS_i) die erste kommutative Prüfsumme (KP1) gebildet
35 wird,

c) für jedes Datensegment (D_j , $j = a \dots z$) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PS_j) gebildet wird,

d) durch eine kommutative Verknüpfung (\oplus) der zweiten Segmentprüfsummen (PS_j) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

e) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

10 14. Anordnung nach einem der Ansprüche 11 bis 13, bei der die Recheneinheit derart eingerichtet ist, daß die Segmentprüfsummen (PS_i , PS_j) nach mindestens einer der folgenden Arten gebildet werden:

- Hashwertbildung,
- 15 - Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

20 15. Anordnung nach einem der Ansprüche 11 bis 14, bei der die Recheneinheit derart eingerichtet ist, daß die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

25 16. Anordnung nach Anspruch 15, bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

30 17. Anordnung nach Anspruch 15, bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

35 18. Anordnung nach einem der Ansprüche 11 bis 17,

bei der die Recheneinheit derart eingerichtet ist, daß die kommutative Verknüpfung (\oplus) die Eigenschaft der Assoziativität aufweist.

- 5 19. Anordnung nach einem der Ansprüche 11 bis 18, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten gesichert werden, deren Datensegmente (D_i) nicht an eine Reihenfolge gebunden sind.
- 10 20. Anordnung nach einem der Ansprüche 11 bis 18, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten gesichert werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.

Zusammenfassung

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehreren Datensegmente
5 gruppiert sind

Es werden Verfahren und Anordnungen zur Bildung einer Prüfsumme und zur Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind, angegeben. Bei
10 dem Verfahren wird für jedes Datensegment eine Prüfsumme gebildet. Die einzelnen Prüfsummen werden unter Verwendung einer kommutativen Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Zur Überprüfung der ersten kommutativen Prüfsumme wird für jedes Datensegment wiederum eine Prüfsumme
15 gebildet und die Prüfsumme wiederum unter Verfahren einer kommutativen Verknüpfung zu einer zweiten kommutativen Prüfsumme verknüpft. Die erste kommutative Prüfsumme und die zweite kommutative Prüfsumme werden auf Übereinstimmung überprüft.

